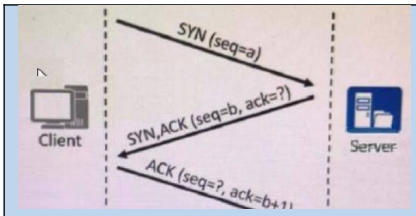
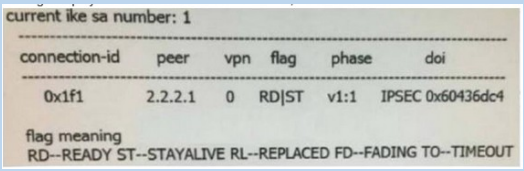
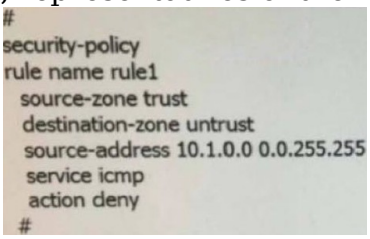
Which of the following guarantees "should detect and protect spam at critical network nodes and maintain upgrades and updates of the spam protection mechanism" in security 2.0?	**Malicious code prevention**	Border protection	Communication transmission	Centralized control
In IPSEC VPN. Which of the following scenarios can be applied by tunnel mode?	**Between security gateways**	Between the host and the host	Between hosts and security gateways	Between tunnel made and transport mode
Which of the following attacks is not a malformed packet attack?	**ICMP unreachable packet attack**	Teardrop attack	Smurf attack	TCP fragmentation attack
After the network attack event occurs, set the isolation area, summary data, and estimated loss according to the plan. Which stage does the above actions belong to the work contents of in the network security emergency response?	**Inhibition phase**	Recovery phase	Detection phase	Preparation stage
Which of the following options does not include the respondents in the questionnaire for safety assessment?	**HR**	Security administrator	Technical leader	Network System Administrator
Which of the following is not included in the Corporate Impact Analysis (BIA)?	**Impact assessment**	Risk identification	Business priority	Accident handling priority
Which of the following is correct for the command to view the number of security policy matches?	**Display security-policy all**	Display firewall session table	Display security-policy count	Count security-policy hit
Which of the following statements about IPSec SA is true?	**IPSec SA is one-way**	Used to generate an encryption key	IPSec SA is two-way	Used to generate a secret algorithm
When the following conditions occur in the VGMP group, the VGMP message will not be sent to the peer end actively?	**Session table entry changes**	Manually switch the active and standby status of the firewall	Firewall service interface failure	Dual hot backup function enabled
In the digital signature process, which of the following is the HASH algorithm to verify the integrity of the data transmission?	**User data**	Receiver public key	Receiver private key	Symmetric key
In the USG series firewall, which of the following commands can be used to query the NAT translation result?	**Display firewall session table**	Display firewall nat translation	Display nat translation	Display current nat
As shown in the figure, a TCP connection is established between client A and server B Which of the following two “T packet numbers should be?	**a+1: a+1**	b+1: b	a: a+1	a+1: a

				
There are various security threats in the use of the server. Which of the following options is not a server security threat?	**Natural disasters**	Malicious programs	Hacking	DDos attack
Which of the following is non-symmetric encryption algorithm?	**DH**	RC4	AES	3DES
Which of the following is correct about the description of SSL VPN?	**Can be used without a client**	May IP encrypt layer	There is a NAT traversal problem	No authentication required
In the USG system firewall, the_____function can be used to provide well-known application services for non-known ports.	**Port mapping**	Packet filtering	MAC and IP address binding	Long connection
Which of the following does not include the steps of the safety assessment method?	**Data analysis**	Manual audit	Penetration test I-	Questionnaire survey
Which of the following descriptions is wrong about IKE SA?	**The encryption algorithm used by user data packets is determined by IKE SA**	IKE is a UDP – based application layer protocol	IKE SA for IPSec SA services	IKE SA is two-way
In the IPSec VPN transmission mode, which part of the data packet is encrypted?	**Transport layer and upper layer data packet**	Network layer and upper layer data packet	New IP packet header	Original IP packet header
Which of the following is not in the quintuple range?	**Source MAC**	Source IP	Destination port	Destination IP
Which of the following attacks is not a cyber-attack?	**MAC address spoofing attack**	IP spoofing attack	ICMP attack	Smurf attack
Which of the following option does not belong to symmetric encryption algorithm?	**RSA**	DES	AES	3DES
Which of the following is the username / password for the first login of the USG series firewall?	**Username admin, password Admin@123**	User name admin, password admin	User name admin, password Admin123	User name admin, password admin@123
Which of the following types of attacks does the DDos attack belong to?	**Traffic attack**	Snooping scanning attack	Malformed packet attack	Special packet attack
Which of the following belongs to Layer 2 VPN technology?	**L2TP VPN**	IPSec VPN	GRE VPN	SSL VPN
Electronic evidence preservation is directly related to the legal	**Message tag**	Encryption technology	Digital signature	Digital certificate technology

effect of evidence, in line with the preservation of legal procedures, and its authenticity and reliability are guaranteed. Which of the following is not an evidence preservation technology?	**tracking technology**		technology	
On Huawei USG series devices, the administrator wants to erase the configuration file. Which of the following commands is correct?	**Reset saved-configuration**	Clear saved-configuration	Reset current-configuration	Reset running-configuration
Winch of the following is the encryption technology used in digital envelopes?	**Asymmetric encryption algorithm**	Symmetric encryption algorithm		
The preservation of electronic evidence is directly related to the legal effect of evidence, and it is in conformity with the preservation of legal procedures, and its authenticity and reliability are guaranteed. Which of the following is not an evidence preservation technique?	**Packet tag tracking technology**	Digital signature technology	Encryption technology	Digital certificate technology
Regarding the HRP master and backup configuration consistency check content, which of the following is not included?	**Next hop and outbound interface of static route**	Authentication Policy	Is the heartbeat interface configured with the same serial number?	NAT policy
The GE1/0/1 and GE1/0/2 ports of the firewall belong to the DMZ. If the area connected to GE1/0/1 can access the area connected to GE1/0/2, which of the following is correct?	**No need to do any configuration**	Need to configure an interzone security policy	Need to configure local to DMZ security policy	Need to configure DMZ to local security policy
Which of the following descriptions about IKE SA is wrong?	**The encryption algorithm used by user data packets is determined by IKE SA**	IKE SA is two-way	IKE is a UDP – based application layer protocol	IKE SA servers for IPSec SA
Which of the following traffic matches the authentication policy triggers authentication?	**Traffic of visitors accessing HTTP services**	The first DNS packet corresponding to the HTTP service data flow	DHCP, BGP, OSPF and LDP packets	Access device or device initiated traffic
Security technology has different approaches at different technical levels and areas. Which of the following devices can be used for	**IPS/IDS equipment**	**Firewall**	**Anti-DDoS equipment**	Vulnerability scanning device

network layer security protection?				
Intrusion prevention system technical characteristics include	**Self-learning and adaptive**	**Real-time blocking**	**Online mode**	Straight road deployment
Which of the following are the hazards of traffic attacks?	**Server downtime**	**Network paralysis**	Data is stolen	The page has been tampered
Which of the following are remote authentication methods?	**HWTACACS**	**RADIUS**	Local	LLDP
Which of the following are the status information that can be backed up by the HRP (Huawei Redundancy Protocol) protocol?	**Dynamic blacklist**	**ServerMap entry**	**Session table**	Routing table
Which of the following information will be encrypted during the use of digital envelopes?	**Symmetric key**	**User data**	Receiver public key	Receiver private key
Which of the following are part of the SSL VPN function?	**File sharing**	**User authentication**	Port scanning	WEB rewriting
Which of the following does the encryption technology support for data during data transmission?	**Confidentiality**	**Integrity**	**Source verification**	Controllability
Which of the following options are supplied by VPN technology to encrypt data messages	**IPSec VPN**	**SSL VPN**	L2TP VPN	GRE VPN
Which of the following are multi-user operating systems?	**Windows**	**LINUX**	**UNIX**	MSDOS
Which of the following options can be used in the advanced settings of Windows Firewall?	**Set connection security rules**	**Restore defaults**	**Set out inbound rules**	**Change notification rules**
Which of the following are the standard port numbers for the FTP protocol?	**21**	**20**	80	23
Which of the following are core elements of the IATF (Information Assurance Technology Framework) model?	**Person**	**Operation**	**Technology**	Environment
Which of the following are in the certification area of IS027001?	**Personnel safety**	**Vulnerability management**	**Access control**	**Business continuity management**
Which of the following 3re the versions of the SNMP protocol?	**SNMPv2c**	**SNMPv3**	**SNMPv1**	SNMPv2b
Which of the following are the characteristics of a symmetric encryption algorithm?	**Key distribution is not secure**	**Fast encryption**	Confidential speed is slow	Key distribution security is high
Through display ike sa to see the result as follows, which	**The first stage ike sa**	**ike is using**	The second stage ipsec sa	ike is using version v2

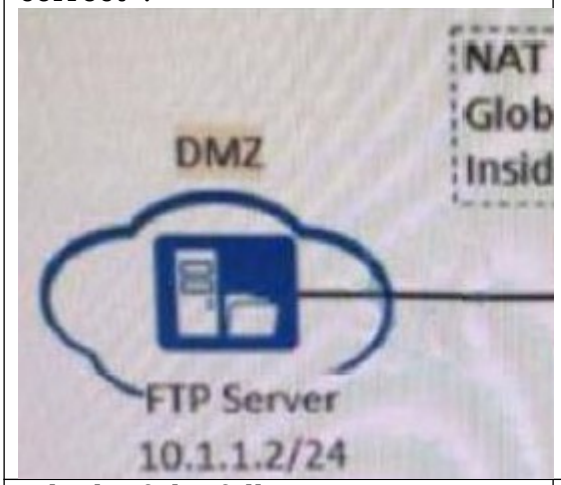
statements are correct? 	**has been successfully established**	**version v1**	has been successfully established	
Which of the following statement about the NAT configuration is wrong?	**The firewall does not support NAPT conversion for ESP and AH packets.**	When there is VoIP service in the network, you do not need to configure NAT ALG	Configure source NAT in -. transparent mode, the firewall does not support easy-ip mode	The IP address in the address pool can overlap with the public IP address of the NAT server
Regarding the firewall security policy, which of the following options are wrong?	**If the security policy is permit, the discarded message will not accumulate the number of hits.**	Adjust the order of security policies without saving the configuration file.	The number of security policy entries of Huawei USG series firewalls cannot exceed 128.	When configuring the security policy name, you cannot reuse the same name
The following security policy command, representatives of the meaning: 	**banned from trust region access to untrust region and the source address is 10.1 0 0/16 segment all the hosts ICMP message**	banned from trust region access to untrust region and the destination address is 10 1 10 10 host ICMP message	banned from trust region access to untrust region and the source address is 10.2.10.10 host to all the hosts ICMP message	banned from trust region access to untrust region and the destination address is 10.1 0 0/16 segment all hosts ICMP message
In L2TP configuration for command Tunnel Name, which statements are correct?	**If do not configure the Tunnel Name, the tunnel name is the name of the local system**	**Used to specify the name of the end of the tunnel**	Must be consistent with Tunnel Name peer configuration	Used to specify the name of the peer tunnel
Against Buffer overflow attacks, which description is correct?	**Buffer overflow attack belongs to the application layer attack behavior**	**Bufter overflow attack ls the most common method of attack software**	**Buffer overflow attack is use of the software system on memory operating**	Buffer overflow attack has nothing to do with operating system's vulnerabilities and architecture

		system's behaviors	**defects, by using high operating permission to run attack code**	
Which of the following descriptions of the firewall fragment cache function are correct?	**For fragmented packets, NAT ALG does not support the processing of SIP fragmented packets.**	**By default, the number of large fragment caches of an IPV4 packet is 32, and the number of large fragmentation buffers of an IPV6 packet is 255**	**By default, the firewall caches fragmented packets**	After the fragmented packet is directly forwarded, the firewall forwards the fragment according to the interzone security policy if it is not the fragmented packet of the first packet
In stateful inspection firewall, when opening state detection mechanism, three-way handshake's second packet (SYN + ACK) arrives the firewall. If there is still no corresponding session table on the firewall, then which of the following statement is correct?	**Packets must not pass through the firewall**	If the firewall security policy allows packets through, then the packets can pass through the firewall	Packets must pass through the firewall, and establishes a session table	If the firewall security policy allows packets through, then creating the session table
About the description about the preemption function of VGMP management, which of the following statements is? wrong?	By default, the preemption delay of the VGMP management group is 40s.	Preemption means that when the faulty primary device recovers, it priority will be restored. At this time, it can regain its own state	After the VRRP backup group is added to the VGMP management group, the original preemption function on the VRRP backup group is invalid.	By default, the preemption function of the VGMP management group is enabled.
Which of the following statement about the NAT is wrong?	For some non-TCP, UDP protocols (such as ICMP, PPTP),	Some application layer protocols earn/ IP address information	Address Translation can follow the needs of users, providing FTP, WWW,	NAT technology can effectively hide the hosts of the LAN. it is an effective network security protection technol

	unable to do the NAT translation	in the data, but also modify the P address information in the data of the upper layer when they are as NAT	Telnet and other services outside the LAN	ogy
Regarding the comparison between windows and Linux, which of the following statements is wrong?	windows is open source, you can do what you want	Windows can be compatible with most software playing most games	Linux is open source code, you can do what you want	Getting started with Linux is more difficult and requires some learning and guidance.
Which of the following is true about firewall security policies?	By default, the security policy only controls unicast packets	By default, the security policy can control unicast packets, broadcast packets, and multicast packets	By default, the security policy can control unicast packets and broadcast packets.	By default, the security policy can control multicast
What are the advantages of address translation techniques included?	Address conversion can block internal network users, improve the safety of internal network	Many host address conversions can make the internal LAN to share an IP address on the Internet	Address conversion can make internal network users (private P address) easy access to the Internet	Address conversion that can handle the IP header of encryption
Which of the following statement about the L2TP VPN of Client-initialized is wrong?	remote users do not need to install VPN client software	After the remote user access to internet, can initiate L2TP tunneling request to the remote LNS directly through the client software	LNS device receives user L2TP connection request, can verify based on user name and password.	LNS assign a private IP address for remot e user
Which of the following description	The	Master/	master/slave	Periodically sends

about the group management for VGMP is wrong?	interface type and number or two firewalls heartbeat port may be different, as long as they can communicate with each other	slave status change of VRRP backup group needs to notify its VGMP management group.	devices exchange packets to understand each other through the heartbeat line, and backup the related commands and status information	Hello packets between VGMP of master/slave firewall
Which of the following statements is wrong about VPN?	VPN technology necessarily involves encryption technology	The generation of VPN technology enables employees on business trips to remotely access internal corporate servers	VPN technology is a technology that multiplexes logica channels or actual physical lines	Virtual private network is cheaper than dedicated line
Which of the following descriptions about windows logs is wrong?	Windows server 2008 system logs stored in the Application.evtx	The application log contains events logged by the application or system program, mainly recording events in the running of the program.	The system log is used to record the events generated by the operating system components, including the crash of the driver, system components and application software, and data	Windows server 2008 security lug is sluied in security.evtx
Regarding the problem that the two-way binding user of the authentication-free method cannot access the network resources, which of the following options are possible reasons?	The authentication-free user does not use the PC with the specified IP/MAC address.	Online users have reached a large value	The authentication-free user and the authenticated user are in the same security zone	The authentication action in the authentication policy is se- to "No credit / free authentication"
Which of the following io true about the description of the firewall?	Depending on the usage scenario, the	In order to avoid single point of	Adding a firewall to the network will	The firewall cannot transparently

	firewall can be deployed in transparent moce or deployed in a three-bedroom mode.	failure. the firewall only supports side-by-side deployment .	inevitably change the topology of the network	access the networ k.
Against IP Spoofing, which of the following description is wrong?	Af-.er IP spoofing attack is successful; the attacker can use forged any IP address to imitate legitimate hast to access to critical information	An attacker would need to cisguise the source IP addresses as trusted hosts, and send the data segment with the SYN flag request for connection	IP spoofing is to use the hosts' normal trust relationship based on the IF address to lau nch it	
ASPF (Application Specific Packet Filter) is a kind of packet filtering based on the application layer, it checks the application layer protocol information and monitor the connection state of the application layer protocol. ASPF by Server Map table achieves a special security mechanism. Which statement about ASPF and Server map table are correct?	ASPF dynamically create and delete filtering rules	ASPF monitors the packets in the process of communica tion	ASPF through server map table realize dynamic to allow multi-channel protocol data to pass	Quintuple server-map entries achieve a similar functionality with session table
Which of the following descriptions about the action and security profile of the security policy are correct?	The security profile must be applied to the security policy that is allowed to take effect.	If the action of the security policy is "prohibited ", the device will discard this traffic, and then no content security check will be perform ed.	The security profile may know: be applied to the security policy that the action is allowed and take effect	If the security policy action is "Allow", the traffic will not match the security profile.
About the descriptions of windows Firewall Advanced Settings, which of the following is wrong?	When setting the stacking rule, both the local port and the	When setting the pop-up rule, both local ports and remote	When setting the stacking rule, only the local port can be restricted, and the	When setting the pop-up rule, only the local port can be restricted, and the remote port cannot be restrict

	remote port can be restricted	ports can be restricted	remote port cannot be restricted	ed
Regarding the relationship and role of VRRPA/GMP/HRP. which of the following statements are correct?	HRP is responsible for data backup during hot standby operation	VRRP is responsible for sending free ARP to direct traffic to the new primary device during active/standby switchover	VGMP is responsible for monitoring equipment failures and controlling fast switching of equipment	VGMP group in the active state may include the VRRP group in the standby state
Which description about disconnect the TCP connection 4 times-handshake is wrong?	when passive close receipt the first FIN. it will send back an ACK, and randomly generated to confirm the serial number	in passive close the sender after the FIN. initiative to close must send back a confirmation, and will confirm the serial number is set to receive serial number 1	initiative to shut down the sender first FIN active closed, while the other received this FIN perform passive shut down	passive closing party end need to send a file to the application the application will close it connection and lead to send a FIN
As shown in the figure, a NAT server application scenario is configured when the web configuration mode is used. Which of the following statements are correct"? 	When configuring an interzone security policy, set the source security zone to Untrust and the target security zone to DMZ	When configuring NAT Server, the internal address is 10 1.1 2 and the external address is 2 00.10.10.1	When configuring an interzone security policy, set the source security zone to DMZ and the target security zone to Untrust	When configuring NAT Server, the internal address is 200.10.10.1 and the external address is 10.1.1.2.
Which of the following statements about Client-Initiated VPN is correct?	A tunnel is established between	Only one L2TP session and	Each tunnel carries multiple L2TP	Each tunnel carries multiple L2TP sessions

	each access user and the LNS	PPP connection are carried in each tunnel	sessions and PPP connections.	and one PPP connection.

.